

EXPRESS MAIL NO. EJ470370785US

CLAIMS:

1 1. A method of securely providing data to a user's system over a web broadcast infrastructure
2 with a plurality of channels, the method comprising the steps of:
3 encrypting the data using a first encrypting key;
4 encrypting the first decrypting key using a second encrypting key;
5 broadcasting promotional metadata related to at least part of the encrypted data on a first
6 web broadcast channel for reception by at least one user's system;
7 broadcasting at least part of the encrypted data over a second broadcast channel; and
8 transferring the encrypted first decrypting key, which has been encrypted with the second
9 encrypting key, to the user's system via a computer readable medium.

1 2. The method as defined in claim 1, wherein the step of broadcasting the promotional
2 metadata includes broadcasting the promotional metadata periodically over a predetermined time
3 interval.

EXPRESS MAIL NO. EJ470370785US

1 The method as defined in claim 1, wherein the step of broadcasting the promotional
2 metadata includes the sub-step of:
3

converting at least the promotional meta data into a format readable by a web browser;

1 4. The method as defined in claim 1, wherein the step of broadcasting at least part of the
2 encrypted data includes broadcasting a schedule of the broadcast time and web broadcast channel
3 for at least part of the encrypted data;

1 5. The method as defined in claim 1, wherein the step of broadcasting at least part of the
2 encrypted data over a second web broadcast channel includes broadcasting the encrypted data
3 in a format compatible with DirecPC™.

1 6. The method as defined in claim 1, wherein the promotional metadata contains a schedule
2 of broadcast times for the data.
3

EXPRESS MAIL NO. EJ470370785US

1 7. A method of securely receiving data on a user's system from a web broadcast infrastructure
2 with a plurality of channels, the method comprising the steps of:
3 receiving promotional metadata from a first web broadcast channel, the promotional
4 metadata related to data available for reception;
5 assembling at least part of the promotional metadata into a promotional offering for review
6 by a user;
7 selecting by a user, data to be received related to the promotional metadata;
8 receiving data from a second web broadcast channel, the data selected from the
9 promotional metadata, and wherein the data has been previously encrypted using a first
10 encrypting key; and
11 receiving the first decrypting key via a computer readable medium, the first decrypting key
12 for decrypting at least some of the data received via the second web broadcast channel.

1 8. The method as defined in claim 7, wherein the step of assembling at least part of the
2 promotional data includes assembling at least part of the promotional data into a format readable
3 by a web browser and wherein the step of selecting includes selecting with a web browser.

1 9. The method as defined in claim 7, wherein the step of selecting includes selecting
2 promotional material that have been previously received and stored on the user's system.

1 10. The method as defined in claim 9, wherein the step of selecting further comprises the sub-
2 steps of:
3 determining the schedule for the next web broadcast of the data selected;
4 setting a trigger to trigger the user's system to receive the next web broadcast on the second
5 channel.

1 11. The method as defined in claim 10, wherein the step of receiving data from a second web
2 broadcast channel, includes receiving the data selected from the promotional metadata on a web
3 broadcast channel and a time provided by the trigger.

Sub A7 > 1 12. The method as defined in claim 7, wherein the step of receiving data from a second web
2 broadcast channel includes receiving data in a format compatible with DirecPC™.

Sub 22 1 13. The method as defined claim 7, wherein the step of receiving data from a second web
2 broadcast channel include the sub-step of:
3 authorizing over a back channel that the user's system is authorized to receive the data
4 selected; and wherein the step of receiving the first decrypting key includes receiving the first
5 decrypting key only if the user's system is authorized to receive the data selected.

1 14. The method as defined claim 7, wherein the step of receiving data from a second web
2 broadcast channel further includes the sub-step of:
3 notifying the user the next time the user starts the user's system a status if the data selected
4 from the promotional metadata has been received on the user's system.

1 15. The method as defined in claim 7, wherein the step of receiving the first decrypting key,
2 includes receiving the first decrypting key that has been encrypted with a second encrypting key.

1 16. The method as defined in claim 15, wherein the step of receiving the first decrypting key
2 includes receiving the first decrypting key over a broadcast stream.

1 17. The method defined in claim 15, wherein the second decrypting key is sent to the user's
2 system from a clearinghouse.

1 18. The method defined in claim 15, wherein the second decrypting key has a timeout
2 provision for decrypting data that has been encrypted with the second encryption key is sent to
3 the user's system from a clearinghouse.

EXPRESS MAIL NO. EJ470370785US

1 19. A system for securely providing data to a user's system over a web broadcast infrastructure
2 with a plurality of channels, the system comprising:
3 a content system;
4 a first public key;
5 a first private key, which corresponds to the first public key;
6 a data encrypting key;
7 a data decrypting key for decrypting data encrypted using the data encrypting key;
8 first data encryption means for encrypting data so as to be decryptable only by the data
9 decrypting key;
10 second data encryption means, using the first public key, for encrypting the data decrypting
11 key;
12 a clearing house;
13 a broadcast center, for broadcasting to one or more user's systems on a first web broadcast
14 channel, promotional metadata related to data being broadcasted on a second web broadcast
15 channel, and broadcasting on the second broadcast channel data encrypted with the data
16 encrypting key;
17 first transferring means for transferring the data decrypting key which has been encrypted
18 to the clearing house, wherein the clearinghouse possesses the first private key;
19 first decrypting means for decrypting the data decrypting key using the first private key;
20 a second public key;
21 a second private key; which corresponds to the second public key;
22 re-encryption means for re-encrypting the data decrypting key using the second public key;
23 second transferring means for transferring the re-encrypted data decrypting key to the user's
24 system, wherein the user's system possesses the second private key; and
25 second decrypting means for decrypting the re-encrypted data decrypting key using the
26 second private key.

1 20. The system as defined in claim 19, wherein the promotional metadata contains a schedule
2 of broadcast times for the data.

EXPRESS MAIL NO. EJ470370785US

1 21. A user's system for securely receiving data from a web broadcast infrastructure with a
2 plurality of channels, comprising:
3 a receiver for receiving promotional metadata from a first web broadcast channel, the
4 promotional metadata related to data available for reception;
5 an interface to an output device for presenting at least part of the promotional metadata for
6 review by a user;
7 an interface to an input device for receiving a selection by a user of the data to be received
8 related to the promotional metadata;
9 a controller for controlling the receiver to receive data from a second web broadcast
10 channel, the data selected from the promotional metadata, and wherein the data has been
11 previously encrypted using a first encrypting key; and
12 an interface for receiving the first decrypting key via a computer readable medium, the first
13 decrypting key for decrypting at least some of the data received via the second web broadcast
14 channel.

1 22. The user's system as defined in claim 21, wherein the output device is a web browser and
2 the input device is coupled to the web browser for receiving a selection by a user.

1 23. The user's system as defined in claim 21, wherein the controller further comprises:
2 a schedule derived from the promotional metadata wherein the schedule is used to control
3 the receiver to receive data from a second web broadcast channel.

1 24. The user's system as defined in claim 21, wherein the receiver is adapted to receive data
2 broadcasted in a format compatible with DirecPC™.